Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) An access point device for a wireless LAN for isolating an end station from a plurality of end stations to support segregation of network traffic between the end station and the plurality of end stations, the access point device serving as a common access point for communication in the wireless LAN, the access point device configured to:

receive a request from said end station that is an association request or a probe request; and

process said request by:

determining for said request a basic service set (BSS) that is unknown to said access point device at the time of receipt of said request by said access point device;

receiving at least one parameter defining said BSS;

establishing said BSS based at least on said at least one parameter;

establishing a security association with said end station within said BSS wherein the security association includes at least two keys, one key for encryption and another key for computing an authentication code; and

sending a response to said end station that includes a BSSID of said established BSS.

2. (Previously presented) The access point device of Claim 1, further configured to provision a plurality of separate LAN segments while providing separate link privacy and integrity for each of said LAN segments.

3-6. (Canceled)

7. (Previously Presented) A method in an access point device for a secure wireless network to support segregation of network traffic among a plurality of stations, each of said stations having a hardware (MAC) address, comprising:

receiving an association request or a probe request from a first station;

determining for said request a basic service set (BSS) that is unknown to said access point device at the time said request was received by said access point device;

receiving at least one parameter which defines said BSS;

establishing said BSS based at least on said at least one parameter, thereby creating the Basic Service Set (BSS) for a subset of said stations;

establishing a security association with each of said end stations within said BSS wherein the security association includes at least two keys, one key for encryption and another key for computing an authentication code; and

sending a response to said end station that includes a BSSID of said established BSS,

wherein stations in said subset belong to said established BSS and share a group security association.

8-50. (Canceled)

53. (Previously presented) The access point device of Claim 1 wherein said request includes an SSID (service set identifier), wherein said at least one parameter is based on said SSID.

54-55. (Canceled)

56. (Currently Amended) A secure wireless network, comprising:

a virtual 802.11 Basic Service Set (BSS);

a plurality of stations in the virtual BSS, each of said stations having a hardware media access control (MAC) address;

all said stations in said virtual BSS sharing a group security association wherein said group security association is an implementation of a MAC security; and

one of said stations in said virtual BSS comprising [[an]] a public access point which is a physical access point.

57. (Previously Presented) The network of claim 56, wherein said implementation of said MAC security comprises said implementation of a secure MAC service.

58. (Previously Presented) The network of claim 57, wherein said implementation of said secure MAC service comprises a MAC Security Key Agreement and a MAC Security Entity.

59. (Previously Presented) The network of claim 57, wherein said group security association comprises using one or more cryptographic methods.

60. (Previously Presented) The network of claim 59, further comprising the one or more cryptographic methods implemented in a security relationship maintained by a MAC Security Key Agreement.

61. (Currently Amended) A method in an access point device for a secure wireless network to support segregation of network traffic among a plurality of stations, each of said stations having a hardware media access control (MAC) address, comprising:

receiving an association request or a probe request from a first station;

determining for said request a basic service set (BSS) that is unknown to said access point device at a time said request was received by said access point device;

receiving at least one parameter which defines said BSS;

establishing said BSS based at least on said at least one parameter, thereby creating said BSS for a subset of said stations; and

sending a response to said end station that includes a BSSID of said established BSS;

wherein stations in said subset belong to said established BSS and share a group security association wherein said group security association is an implementation of a MAC security wherein said implementation of said MAC security comprises said implementation of a secure MAC service.

62. (Canceled)

63. (Currently Amended) The method of claim [[62]]61, wherein said implementation of said secure MAC service comprises a MAC Security Key Agreement and a MAC Security Entity.

64. (Currently Amended) The method of claim [[62]]61, wherein said group security association comprises using one or more cryptographic methods.

65. (Previously Presented) The method of claim 64, further comprising the one or more cryptographic methods implemented in a security relationship maintained by a MAC Security Key Agreement.

66. (Previously Presented) An access point for segregating traffic among a plurality of end stations, comprising:

one or more storage units configurable to store:

a frame having a cryptographic authentication code;

the frame having a source media access control (MAC) address to determine a preliminary VLAN classification when the frame carries a null virtual LAN ID;

the frame having a virtual LAN ID (VID) as the preliminary VLAN classification when the frame carries the VID;

a table of security associations providing a cryptographic authentication code key based on the preliminary VLAN classification wherein the cryptographic authentication code key is used to recompute a new cryptographic authentication code over a payload of the frame;

the new cryptographic authentication code compared with the cryptographic authentication code;

the preliminary VLAN classification implemented as a final VLAN classification when the new cryptographic authentication code and the cryptographic authentication code match, wherein the frame is decrypted; and

the preliminary VLAN classification not implemented as the final VLAN classification when the new cryptographic authentication code and the cryptographic authentication code do not match, wherein the frame is discarded.

67. (Previously Presented) The access point of claim 66, wherein the access point is configurable to perform an authentication operation that generates the authentication code key.

68. (Previously Presented) The access point of claim 66, wherein the new cryptographic authentication code is recomputed over the payload using a cryptographic message digest algorithm determined during an initial authentication operation.

69. (Previously Presented) The access point of claim 66, wherein the final VLAN classification is used as a value of a VLAN classification parameter of any corresponding data request primitives.

70. (Previously Presented) The access point of claim 66, wherein the cryptographic authentication code or the new cryptographic authentication code uniquely identifies the VLAN.